1. (currently amended) A method for identifying or disabling at least one traitor receiver with at least one associated unique, compromised decryption key in a broadcast encryption system, comprising:

receiving a set of subsets derived from a tree defining leaves, each leaf representing a respective receiver;

identifying at least one traitor subset from the set of subsets as containing at least one leaf representing a traitor receiver; ~~and~~

using the traitor subset, identifying or disabling the traitor receiver; and

determining whether the traitor subset represents at least two traitor receivers, and if so, dividing the traitor subset into two child sets.

2. (canceled).

3. (currently amended) The method of Claim ~~2~~ 1, further comprising determining whether the traitor subset is a member of a frontier set, and if so, removing a complementary subset from the frontier set.

4. (original) The method of Claim 1, wherein the act of identifying or disabling includes encoding plural subsets of the set of subsets with a false key.

5. (original) The method of Claim 4, further comprising executing a binary search on the set of subsets using probabilities.

6. (original) The method of Claim 5, wherein the binary search ends by determining that the difference between a probability p_j of decrypting a message when the first j subsets contain the false key and a probability p_{j-1} of decrypting a message when the first j-1 subsets contain the false key is at least equal to a predetermined probability.

7. (original) The method of Claim 6, wherein the traitor subset is identified when $| p_{j-1}-p_j | > p/m$, wherein m is the number of subsets in the set of subsets.

8. (original) The method of Claim 1, wherein the set of subsets is generated by:

assigning each receiver in a group of receivers respective private information I_u;

selecting at least one session encryption key K;

partitioning receivers not in a revoked set R into a set of disjoint subsets $S_{i1},\ldots,S_{im}$ having associated subset keys $L_{i1},\ldots,L_{im}$; and

encrypting the session key K and the false key with the subset keys $L_{i1},\ldots,L_{im}$.

9. (original) The method of Claim 8, wherein the tree includes a root and plural nodes, each node having an associated key, and wherein each receiver is assigned keys from all nodes in a direct path between a leaf representing the receiver and the root.

10. (original) The method of Claim 8, wherein the tree includes a root and plural nodes, each node associated with a set of labels, and wherein each receiver is assigned labels from all nodes hanging from a direct path between the receiver and the root but not from nodes in the direct path.

11. (original) The method of Claim 10, wherein the revoked set R defines a spanning tree, and wherein the method includes:

initializing a cover tree T as the spanning tree;

iteratively removing nodes from the cover tree T and adding nodes to the cover tree T until the cover tree T has at most one node.

12. (original) A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer, comprising:

logic means for accessing a tree to generate a set of subsets of the tree, the tree including leaves representing at least one traitor device characterized by a compromised key;

logic means for encrypting a false key j times and for encrypting a session key m-j times, wherein m is a number of subsets in the set of subsets;

logic means responsive to the means for encrypting for identifying a traitor subset; and

logic means for using the traitor subset to identify or disable the traitor device.

13. (currently amended) The computer program device of Claim 12, further comprising:

logic means for determining whether the traitor subset represents at least ~~one~~ two traitor devices, and if so, dividing the traitor subset into two child sets.

14. (original) The computer program device of Claim 13, further comprising logic means for determining whether the traitor subset is a member of a frontier set, and if so, removing a complementary subset from the frontier set.

15. (original) The computer program device of Claim 12, further comprising logic means for executing a binary search on the set of subsets using probabilities.

16. (original) The computer program device of Claim 15, wherein the binary search ends by determining that the difference between a probability p_j of decrypting a message when the first j subsets contain the false key and a probability p_{j-1} of decrypting a message when the first j-1 subsets contain the false key is at least equal to a predetermined probability.

17. (original) The computer program device of Claim 16, wherein the traitor subset is identified when $| p_{j-1}-p_j | > p/m$, wherein m is the number of subsets in the set of subsets.

18. (original) The method of Claim 12, wherein the set of subsets is generated by logic means including:

logic means for assigning each receiver in a group of receivers respective private information L_u;

logic means for selecting at least one session encryption key K;

logic means for partitioning receivers not in a revoked set R into a set of disjoint subsets $S_{i1},\ldots S_{im}$ having associated subset keys $L_{i1},\ldots,L_{lm}$; and

logic means for encrypting the session key K and the false key with the subset keys $L_{i1},\ldots,L_{im}$.

19. (original) The computer program device of Claim 18, wherein the tree includes a root and plural nodes, each node having an associated key, and wherein each receiver is assigned keys from all nodes hanging from a direct path between the receiver and the root but not from nodes in the direct path.

20. (original) A computer programmed with instructions to cause the computer to execute method acts including:

using a false key to encode plural subsets representing stateless receivers, at least one traitor receiver of which is associated with at least one compromised key that has been obtained by at least one pirate receiver; and

using the pirate receiver or a clone thereof, determining the identity of the traitor receiver, or rendering the pirate receiver or clone thereof useless for decrypting data using the compromised key.

21. (original) The computer of Claim 20, wherein the subsets define a set of subsets, and the method acts undertaken by the computer further include:

receiving the set of subsets derived from a tree defining leaves, each leaf representing a respective receiver;

identifying at least one traitor subset from the set of subsets as containing at least one leaf representing the traitor receiver; and

using the traitor subset, identifying the traitor receiver.

22. (currently amended) The computer of Claim 21, wherein the method acts undertaken by the computer further comprise:

determining whether the traitor subset represents at least ~~one~~ two traitor receivers, and if so, dividing the traitor subset into two child sets.

23. (original) The computer of Claim 22, wherein the method acts undertaken by the computer further comprise determining whether the traitor subset is a member of a frontier set, and if so, removing a complementary subset from the frontier set.

24. (original) The computer of Claim 21, wherein the act of identifying includes:

encoding plural subsets of the set of subsets with the false key.

25. (original) The computer of Claim 24, wherein the method acts undertaken by the computer further comprise executing a binary search on the set of subsets using probabilities.

26. (original) The computer of Claim 25, wherein the binary search ends by determining that a probability p_j of decrypting a message when the first j subsets contain the false key is at least equal to a predetermined probability.

27. (original) The computer of Claim 26, wherein the traitor subset is identified when $| p_{j-1}-p_j | > p/m$, wherein m is the number of subsets in the set of subsets.

28. (original) The computer of Claim 21, wherein the set of subsets is generated by:

assigning each receiver in a group of receivers respective private information I_u;

selecting at least one session encryption key K;

partitioning receivers not in a revoked set R into a set of disjoint subsets $S_{i1},\ldots S_{im}$ having associated subset keys $L_{i1},\ldots,L_{im}$; and

encrypting the session key K and the false key with the subset keys $L_{i1},\ldots,L_{im}$, wherein the tree includes a root and plural nodes, each node being associated with a set of labels, and wherein each receiver is assigned labels from all nodes hanging from a direct path between the receiver and the root but not from nodes in the direct path.

29. (original) The method of Claim 1, further comprising identifying or disabling plural traitor receivers embodied in a clone.

30. (original) The method of Claim 1, wherein the act of identifying or disabling includes encoding the first j subsets of the set of subsets with a false key.